

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

United States of America

v.

Michael Deangelo Johnson-Brown

Case: 4:21-mj-30525

Judge: Curtis Ivy, Jr.

Filed: 11-08-2021

IN RE SEALED MATTER (kcm)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.


On or about the date(s) of _____ (see below) _____ in the county of _____ Genesee _____ in the
 _____ Eastern _____ District of _____ Michigan _____, the defendant(s) violated:

| <i>Code Section</i> | <i>Offense Description</i> |
|--|----------------------------|
| 18 U.S.C. § 1344(1) - from 5/24/18, through at least 7/11/19 | Bank fraud; |
| 18 U.S.C. § 1029(a)(2) - from about 5/24/18 through 5/23/19; and | Access device fraud; and |
| 18 U.S.C. § 1028A(a)(1) - from about 5/24/18 through 7/11/19 | Aggravated identity theft |

This criminal complaint is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.Sworn to before me and signed in my presence
and/or by reliable electronic means.Date: November 8, 2021City and state: Flint, Michigan



 Complainant's signature

Scot Bryan, Special Agent-USSS

Printed name and title



 Judge's signature

Curtis Ivy, Jr., United States Magistrate Judge

Printed name and title

Affidavit

I, Scot Bryan, being duly sworn, state the following is true and accurate to the best of my knowledge and belief.

Introduction

1. I am a Senior Special Agent (SSA) with the U.S. Secret Service (USSS) within the Department of Homeland Security and have been so employed since February 2002. I am currently assigned to the Saginaw, Michigan, Resident Office. In preparation for my employment with the USSS, I successfully completed criminal investigator training at the Federal Law Enforcement Training Center in Glynco, Georgia. I also successfully completed training with the USSS at the James J. Rowley Training Center in Beltsville, Maryland. Before working for the USSS, I served for five years as a state trooper with the New Hampshire State Police. The combination of both my current and former employment has provided me with training and experience in criminal investigation, interviewing suspects, and financial crimes. In June 2004, I successfully completed the Federal Law Enforcement Training Center's Treasury Computer Forensics Training Program in Glynco, Georgia. I have since received advance training from Access Data and Guidance Software. I am A+ Certified with a basic knowledge of computer hardware and software. I have conducted multiple computer forensic examinations since completing this training.

2. I make this affidavit in support of a criminal complaint and arrest warrant charging Michael Deangelo Johnson-Brown with violating 18 U.S.C. § 1344(1), bank fraud; 18 U.S.C. § 1029(a)(2), access fraud device; and 18 U.S.C. § 1028A(a)(1), aggravated identity theft. The facts in this affidavit are based upon personal knowledge from my participation in this investigation and information received from bank investigators, other law enforcement personnel and their reports and records, witness accounts, and business records. The information outlined below is provided for the limited purpose of establishing probable cause, and does not contain all details or facts that exist pertaining to the investigation. The transactions described below set forth only some—but not all—of the fraudulent conduct identified and under investigation.

Probable Cause

3. As background, on March 9, 2018, Chris Allen, Corporate Investigator for Fifth Third Bank, informed the USSS about credit card fraud and identity theft emanating from Flint, Michigan. Allen advised fraud had occurred in the name of Michael Brown. Allen advised that Fifth Third Bank customers with the same or similar names to Michael Brown were, for the most part, the reported victims. Allen reported that the fraudulent scheme involved Michael Deangelo Johnson-Brown using the victims' stolen personal identification information, specifically, their name and social security number, to open checking and credit accounts at

Fifth Third Bank. Based on Johnson-Brown's false representations, Fifth Third Bank opened checking accounts and credit accounts for Johnson-Brown, who provided a mailing address in the Flint area to receive the cards and statements. At the time of the application, the victims were unaware that an account had been opened in their names with their social security numbers at Fifth Third Bank, and in some cases, the victims had never had a Fifth Third Bank account.

4. In June 2018, Bryan Rozanski, Citibank Lead Investigator, informed the USSS that persons had committed substantial fraud through identity theft in Flint and surrounding areas. Rozanski reported that merchant credit accounts, backed by Citibank, were applied for online from the Flint area, and the accounts were then used in Michigan and Ohio. Rozanski explained that these accounts were fraudulently applied for in the names of real persons whose names were Michael Brown or a similar derivative. In applying for these merchant credit accounts, Johnson-Brown used the name (often Michael Brown or a derivative thereof), the social security number, the address, and telephone number of another person. Based on Johnson-Brown's false representations, Citibank extended a line of credit to Johnson-Brown, who at times used these accounts before the victims were aware the accounts had been activated. Johnson-Brown used some of these accounts before physically obtaining the card by imputing the identity-theft victim's social security number into the merchant's card reader. In these instances, the victim was

unaware an account had been created with their personal information until they received the physical card and statement. Rozanski provided information captured by Citibank, including the victims' personal identification information, the internet protocol address used in making the credit application, and the specific device identification number used to make the credit application.

5. In 2016, United States Postal Inspector Andre Brown received information from Synchrony Bank investigator, Bonita Walker, regarding fraudulent activity with Synchrony accounts in the Flint area. Synchrony reported that the accounts were not all in the same name, but several displayed a common mailing address of **** Magnolia Drive, Mount Morris, Michigan. This specific address was displayed as Johnson-Brown's address on his Michigan driver's license during the timeframe of the fraudulent transactions described below. Michigan Secretary of State records show that Johnson-Brown's listed address changed in June of 2021. Several, but not all, of the accounts were in the name of Michael Brown. In applying for these merchant credit accounts, Johnson-Brown used the name, the social security number, the address, and telephone number of other persons. Based on Johnson-Brown's false representations, Synchrony Bank extended a line of credit and mailed a physical card to Johnson-Brown, who at times used these accounts before the victims were aware the accounts had been activated. Walker

provided information captured by Synchrony Bank, including the victims' personal identification information.

6. Law enforcement personnel obtained video surveillance and still photographs of numerous fraudulent transactions. United States Postal Inspector Andre Brown reviewed this evidence and identified Johnson-Brown as the person making the fraudulent transactions described below. Postal Inspector Brown identified Johnson-Brown from previous criminal investigations involving Johnson-Brown. During some of the fraudulent transactions, Johnson-Brown identified himself to merchants by presenting his valid Michigan driver's license.

7. I have reviewed video of several fraudulent transactions described below.

8. Around 10:15 a.m. on May 24, 2018, Johnson-Brown made a fraudulent transaction at a Home Depot store, located at 2205 East M21 in Owosso, Michigan. This Home Depot is in Shiawassee County, within the Eastern District of Michigan. Both Home Depot and Citibank reported this as a fraudulent transaction. At this place and time, Johnson-Brown applied for a credit card online through Citibank. In doing so, Johnson-Brown used the name "Michael Brown" and a social security number ending in the numbers 2445. This social security number belongs to a Michael Brown that lives in Ridgely, Maryland. Michael Brown from Maryland submitted an affidavit of fraud to Citibank wherein he confirmed that he did not apply for or authorize the application of a Home Depot

credit card in Michigan. Based on the information Johnson-Brown provided, Citibank approved a credit account ending in numbers 1220. This transaction affected interstate commerce as Citibank approved this transaction in Omaha, Nebraska. Using this credit account number, Johnson-Brown then bought various items at Home Depot, totaling \$5,566.01. Home Depot video surveillance footage shows Johnson-Brown making this transaction. Since this fraudulent transaction on May 24, 2018, Johnson-Brown has not made payments to Home Depot or Citibank related to this account.

9. The next day, Johnson-Brown made another fraudulent transaction at a Home Depot store, located at 3860 State Street in Bay City, located within the Eastern District of Michigan. Both Home Depot and Citibank reported this as a fraudulent transaction. At this place and time, Johnson-Brown applied for a credit card online through Citibank. In doing so, Johnson-Brown used the name “Michael Brown” and a social security number ending in the numbers 8563. This social security number belongs to a Michael Brown that lives in Eagle, Wisconsin. Michael Brown from Wisconsin submitted an affidavit of fraud to Citibank wherein he confirmed that he did not apply for or authorize the application of a Home Depot credit card in Michigan. Based on the information Johnson-Brown provided, Citibank approved a credit account ending in numbers 4090. This transaction affected interstate commerce as Citibank approved this transaction in

Omaha, Nebraska location. Using this credit account, Johnson-Brown then bought various items at Home Depot, totaling \$6,345.16. Home Depot video surveillance footage shows Johnson-Brown making this transaction. The receipt for this transaction recorded the date, the total amount of items purchased, and the last four digits (9325) of Johnson-Brown's Michigan driver's license. Since this fraudulent transaction on May 25, 2018, Johnson-Brown has not made payments to Home Depot or Citibank related to this account.

10. On September 19, 2018, Johnson-Brown made a fraudulent transaction at ABC Warehouse, located at 4247 Miller Road in Flint Township, within the Eastern District of Michigan. Both ABC Warehouse and Synchrony Bank reported this as a fraudulent transaction. At this place and time, Johnson-Brown applied for a credit card online through Synchrony Bank. In doing so, Johnson-Brown used the name "Michael Brown" and a social security number ending in the numbers 5037. According to Synchrony Bank, this social security number belongs to a Michael Brown that lives in Henderson, Nevada. A law enforcement agent later interviewed Michael Brown from Nevada and he confirmed that he did not apply for an ABC Warehouse credit card in Michigan. Based on the information Johnson-Brown provided, Synchrony Bank approved a credit account ending in numbers 1364. This transaction affected interstate commerce as Synchrony Bank approved this transaction in Omaha, Nebraska location. Using this credit account number,

Johnson-Brown then bought various items at ABC Warehouse, totaling \$9,671.41. ABC Warehouse video surveillance footage shows Johnson-Brown buying these items and an ABC Warehouse employee photocopied Johnson-Brown's Michigan driver license for this transaction. Since this fraudulent transaction on September 19, 2018, Johnson-Brown has not made payments to ABC Warehouse or Synchrony Bank related to this account.

11. In the morning of May 1, 2019, Johnson-Brown made a fraudulent transaction at Belle Tire, located at 6066 South Saginaw Street in Grand Blanc, within the Eastern District of Michigan. Both Belle Tire and Citibank reported this as a fraudulent transaction. At this place and time, Johnson-Brown applied for a credit card online through Citibank. In doing so, Johnson-Brown used the name "Michael Brown" and a social security number ending in the numbers 7107. According to Citibank, this social security number belongs to a Michael Brown that lives in Granby, Connecticut. A law enforcement agent later interviewed Michael Brown from Connecticut and he confirmed that he did not apply for a Belle Tire credit card in Michigan. Based on the information Johnson-Brown provided, Citibank approved a credit account ending in numbers 9202. This transaction affected interstate commerce as Citibank approved this transaction in Omaha, Nebraska. Using this credit account number, Johnson-Brown then bought various items at Belle Tire, totaling \$1,093.92. A Belle Tire employee, Ryan

Lindsay, identified Johnson-Brown during a photo lineup presented by Postal Inspector Andre Brown. Since this fraudulent transaction on May 1, 2019, Johnson-Brown has not made payments to Belle Tire or Citibank related to this account.

12. On July 11, 2019, Johnson-Brown made a fraudulent transaction at the Home Depot located at 1500 Summit Street, Lapeer, Michigan. This Home Depot is in Lapeer County, within the Eastern District of Michigan. Both Home Depot and Citibank reported this as a fraudulent transaction. At this place and time, Johnson-Brown applied for a credit card online through Citibank. In doing so, Johnson-Brown used the name “Michael Brown” and a social security number ending in the numbers 0776. This social security number belongs to a Michael Brown that lives in Windsor, Colorado. A law enforcement agent later interviewed Michael Brown from Colorado and he confirmed that he did not apply for a Home Depot credit card in Michigan. Based on the information Johnson-Brown provided, Citibank approved a credit account ending in numbers 6845. This transaction affected interstate commerce as Citibank approved this transaction in Omaha, Nebraska. Using this credit account number, Johnson-Brown then bought various items at Home Depot, totaling \$8,087.80. Home Depot video surveillance footage shows Johnson-Brown making this transaction. The receipt for this transaction recorded Johnson-Brown’s Michigan driver’s license number on it. Since this

fraudulent transaction on July 11, 2019, Johnson-Brown has not made payments to Home Depot or Citibank related to this account.

13. About five hours later this same day, Johnson-Brown made a fraudulent transaction at the Home Depot located at 3132 Bueker Drive in Saginaw, within the Eastern District of Michigan. Both Home Depot and Citibank reported this as a fraudulent transaction. Using the credit account number (ending in numbers 6845) that he fraudulently obtained earlier in the day, Johnson-Brown bought various items at Home Depot, totaling \$2,421.15. Home Depot video surveillance footage shows Johnson-Brown making this transaction. The receipt for this transaction recorded Johnson-Brown's Michigan driver's license number on it. Since this fraudulent transaction on July 11, 2019, Johnson-Brown has not made payments to Home Depot or Citibank related to this account.

14. After reviewing Johnson-Brown's criminal history and other records, I know that his actual social security number ends in 738 and his Michigan driver's license ends in 325. Based on records provided by Citibank and Synchrony, I know that Johnson-Brown applied for credit—and received approval—using the valid names and social security numbers of different persons who happen to have the same or similar name.

15. I know, based upon information provided by Citibank and Synchrony that both financial institutions are federally insured through FDIC and were so insured during the times set forth above.

16. Under 18 U.S.C. § 1029(e)(1)&(3), I know that the term “access device” means any card, plate, code, account number, electronic serial number . . . or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value[.]


Under this same section, I know that the term “unauthorized access device” means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud. Under 18 U.S.C. § 1028(d)(7)(A), I know that the term “means of identification” includes the name and social security number of another person that may be used, alone or in conjunction with any other information, to identify a specific person. Under 18 U.S.C. § 1028A(c)(4), I know that access device fraud is an enumerated felony for aggravated identity theft. Under 18 U.S.C. § 1028A(c)(5), I know that bank fraud is an enumerated felony for aggravated identity theft.

17. Based on the foregoing, I have probable cause to believe that from about May 24, 2018, through at least July 11, 2019, in the Eastern District of Michigan and elsewhere, Michael Deangelo Johnson-Brown knowingly executed a scheme to defraud a financial institution of money by means of false representations with

the intent to deceive and deprive the financial institution of something of value, in violation of 18 U.S.C. § 1344(1), bank fraud.

18. Based on the foregoing, I have probable cause to believe that from about May 24, 2018, through May 23, 2019, in the Eastern District of Michigan and elsewhere, Michael Deangelo Johnson-Brown knowingly and with intent to defraud used one or more unauthorized access devices and by doing so obtained items of value exceeding \$1000 during this period, in violation of 18 U.S.C. § 1029(a)(2), access device fraud.

19. Based on the foregoing, I have probable cause to believe that from about May 24, 2018, through July 11, 2019, in the Eastern District of Michigan and elsewhere, Michael Deangelo Johnson-Brown knowingly used, without lawful authority, a means of identification of another person during and in relation to his commission of bank fraud and access device fraud, as described above, in violation of 18 U.S.C. § 1028A(a)(1), aggravated identity theft.


Scot Bryan
Senior Special Agent, U.S. Secret
Service

Sworn and subscribed to before me and/or by reliable electronic means on
November 8, 2021
_____.



Curtis Ivy, Jr.
United States Magistrate Judge